TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 345, Number 1, September 1994

A FAMILY OF REAL 2^n-TIC FIELDS

YUAN-YUAN SHEN AND LAWRENCE C. WASHINGTON

ABSTRACT. We study the family of polynomials

$$P_n(X\,;a) = \Re((X+i)^{2^n}) - \frac{a}{2^n}\Im((X+i)^{2^n})$$

and determine when $P_n(X\,;a)$, $a \in \mathbb{Z}$, is irreducible. The roots are all real and are permuted cyclically by a linear fractional transformation defined over the real subfield of the 2^nth cyclotomic field. The families of fields we obtain are natural extensions of those studied by M.-N. Gras and Y.-Y. Shen, but in general the present fields are non-Galois for $n \geq 4$. From the roots we obtain a set of independent units for the Galois closure that generate an "almost fundamental piece" of the full group of units. Finally, we discuss the two examples where our fields are Galois, namely $a = \pm 2^n$ and $a = \pm 2^4 \cdot 239$.

1. INTRODUCTION

One method of constructing cyclic extensions of $\mathbb{Q}$ is the following. Start with $M \in \mathrm{PGL}_2(\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(X))$ of finite order and let $\mathbb{Q}(T)$ be its fixed field. By specialization, one obtains the desired cyclic extensions. For example, the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ yields the family of cyclic cubic polynomials $X^3 - aX^2 - (a+3)X - 1$, named the "simplest cubic fields" by Shanks [11]. Similarly, the matrices $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ yield the polynomials $X^2 - aX - 1$ and $X^4 - aX^3 - 6X^2 + aX + 1$, respectively. The latter family has been studied by M.-N. Gras [4]. There is also a family of sextic polynomials arising from the matrix $\left(\begin{smallmatrix} 1 & -1 \\ 1 & 2 \end{smallmatrix}\right)$ of M.-N. Gras [3]. However, it is easy to see that there are no elements of $\mathrm{PGL}_2(\mathbb{Q})$ of finite orders other than $1, 2, 3, 4, 6$. In [13], one of the authors of the present paper used the matrix $\left(\begin{smallmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{smallmatrix}\right)$ of order 8 in $\mathrm{PGL}_2(\mathbb{Q}(\sqrt{2}))$, where $\varepsilon = \sqrt{2}+1$, and showed that in some cases it is possible to obtain cyclic extensions of $\mathbb{Q}$ of degree 8. In the present paper, we consider transformations of higher 2-power order and obtain a family of fields of degree 2^n for each $n \geq 1$. These fields are non-Galois in general, though they lift to cyclic extensions over the cyclotomic field $\mathbb{Q}(\zeta_{2^n})$, a fact that plays an important role in studying their properties.

Received by the editors June 7, 1993 and, in revised form, February 2, 1994.

1991 *Mathematics Subject Classification*. Primary 11R21; Secondary 11R09, 11R18, 11R20, 11R27.

Key words and phrases. 2^n-tic fields, units.

A key step in constructing our fields rests on the following observation (see [13]):

$$X^2 - aX - 1 = \Re((X+i)^2) - \frac{a}{2}\Im((X+i)^2),$$
$$X^4 - aX^3 - 6X^2 + aX + 1 = \Re((X+i)^4) - \frac{a}{4}\Im((X+i)^4)$$

and similarly for the octic fields of [13]. In general, define

$$P_n(X;a) = \Re((X+i)^{2^n}) - \frac{a}{2^n}\Im((X+i)^{2^n}).$$

It turns out that these polynomials $P_n(X;a)$ generate the fields of degree 2^n, and their roots are permuted cyclically by the transformations mentioned above. We determine exactly when $P_n(X;a)$, $a \in \mathbb{Z}$, is irreducible. This of course reduces to Diophantine questions. It is amusing to note that we encounter the equation $2w^4 = y^2 + 1$ considered by Ljunggren [9, 14], and its (perhaps unexpected) integer point $(w, y) = (13, 239)$.

One reason for studying the "simplest fields" is that the roots of the polynomials yield explicit units that often generate subgroups of small index in the full groups of units [2, 3, 4, 5, 6, 7, 10, 11, 12, 13]. In the present situation, since the extensions we obtain are non-Galois and therefore contain few roots, we are forced to consider the Galois closure, in which case we cannot hope to obtain a maximal set of independent units as roots of our polynomials. However, we show that the group S of units generated by the roots is an "almost fundamental piece" of the unit group in the sense that if $E_1 \supseteq S$ is a subgroup of the full unit group and $[E_1 : S]$ is finite, then this index is bounded uniformly as the parameter for the family varies, under certain mild restrictions.

Acknowledgment. The authors would like to thank the referee for very carefully reading the manuscript and for simplifying the proof of Lemma 2.

2. Construction of the 2^n-tic polynomials

Let $R_n(X) = \Re(X+i)^{2^n}$ and let $I_n(X) = \Im(X+i)^{2^n}$. Then

$$(X+i)^{2^n} = R_n(X) + iI_n(X),$$

and hence

$$R_0(X) = X, \qquad I_0(X) = 1.$$

Observe that

$$\begin{aligned}(X+i)^{2^n} &= ((X+i)^{2^{n-1}})^2 = (R_{n-1}(X) + iI_{n-1}(X))^2 \\ &= (R_{n-1}^2(X) - I_{n-1}^2(X)) + i(2R_{n-1}(X)I_{n-1}(X)),\end{aligned}$$

and we obtain the following recursion formulas:

(1) $$R_n(X) = R_{n-1}^2(X) - I_{n-1}^2(X),$$

(2) $$I_n(X) = 2R_{n-1}(X)I_{n-1}(X).$$

Therefore, the next few $R_n(X)$ and $I_n(X)$ are

$$R_1(X) = R_0^2 - I_0^2 = X^2 - 1, \qquad I_1(X) = 2R_0I_0 = 2X,$$
$$R_2(X) = R_1^2 - I_1^2 = X^4 - 6X^2 + 1, \qquad I_2(X) = 2R_1I_1 = 4X(X^2-1),$$

$$R_3(X) = X^8 - 28X^6 + 70X^4 - 28X^2 + 1,$$
$$I_3(X) = 8X(X^2 - 1)(X^4 - 6X^2 + 1).$$

By induction, we can express the polynomials $R_n(X)$ and $I_n(X)$ in terms of the polynomials $R_j(X)$, $0 \leq j < n$, as follows.

$$I_n(X) = 2^n \prod_{j=0}^{n-1} R_j(X), \qquad n \geq 1; \tag{3}$$

$$R_n(X) = R_{n-1}^2(X) - \left(2^{n-1} \prod_{j=0}^{n-2} R_j(X)\right)^2, \qquad n \geq 2. \tag{4}$$

Applying induction via (4), we have that the polynomials $R_0(X)$, $R_1(X)$, $R_2(X), \dots, R_n(X)$ are pairwise relatively prime, and hence by (3), the polynomials $R_n(X)$ and $I_n(X)$ are also relatively prime. We record this in the following.

Lemma 1. *For any given $n \in \mathbb{Z}^+$, the polynomials $R_0(X), R_1(X), R_2(X), \dots,$ $R_n(X)$ are pairwise relatively prime, and hence the polynomials $R_n(X)$ and $I_n(X)$ are also relatively prime.*

Our 2^n-tic polynomial is of the form

$$P_n(X; a) = R_n(X) - \frac{a}{2^n} I_n(X), \qquad \text{where } a \in \mathbb{Z}. \tag{5}$$

From (3) we see that $P_n(X; a) \in \mathbb{Z}[X]$. From (1) and (2), the right-hand side of (5) becomes

$$R_{n-1}^2(X) - \frac{a}{2^{n-1}} R_{n-1}(X) I_{n-1}(X) - I_{n-1}^2(X),$$

which is a quadratic polynomial in the variables $R_{n-1}(X)$ and $I_{n-1}(X)$. It can be factored into the product

$$\left(R_{n-1}(X) - \frac{a + \sqrt{a^2 + 4^n}}{2^n} I_{n-1}(X)\right) \left(R_{n-1}(X) - \frac{a - \sqrt{a^2 + 4^n}}{2^n} I_{n-1}(X)\right).$$

Therefore the polynomial $P_n(X; a)$ factors over the field $\mathbb{Q}(\sqrt{a^2 + 4^n})$ in the following way:

$$P_n(X; a) = P_{n-1}\left(X; \frac{a + \sqrt{a^2 + 4^n}}{2}\right) P_{n-1}\left(X; \frac{a - \sqrt{a^2 + 4^n}}{2}\right). \tag{6}$$

On the other hand, from (3), we may write the 2^n-tic polynomial $P_n(X; a)$ in terms of the polynomials $R_j(X)$'s as follows:

$$P_n(X; a) = R_n(X) - a \prod_{j=0}^{n-1} R_j(X). \tag{7}$$

Putting (4) and (7) together, we have for $n \geq 2$ the following expression:

$$P_n(X; a) = R_{n-1}^2(X) - aR_{n-1}(X) \prod_{j=0}^{n-2} R_j(X) - 2^{2n-2} \left(\prod_{j=0}^{n-2} R_j(X)\right)^2. \tag{8}$$

3. Basic properties of the 2^n-tic polynomials

As expected, the 2^n-tic polynomial $P_n(X; a)$ has 2^n distinct real roots, which are units in the ring of algebraic integers.

Theorem 1. (a) *For $a \in \mathbb{Z}$, the 2^n-tic polynomial $P_n(X; a)$ has 2^n distinct real roots. In particular, $R_n(X) = P_n(X; 0)$ has 2^n distinct real roots.*

(b) *Let ε be any root of $R_{n-1}(X)$. The matrix $M = \left(\begin{smallmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{smallmatrix}\right)$ has order 2^n in* $\mathrm{PGL}_2(\mathbb{R})$. *The transformation*

$$\theta \mapsto \frac{\varepsilon\theta - 1}{\theta + \varepsilon}$$

permutes cyclically the roots of $P_n(X; a)$.

Proof. We first use induction on n to show that there is at least one real root. This is obvious for $n = 0, 1$, so let $n \geq 2$ and assume this is true for $n - 1$. Let ε be any root of $R_{n-1}(X)$. By (8) we have

$$\begin{aligned} P_n(\varepsilon; a) &= R_{n-1}^2(\varepsilon) - aR_{n-1}(\varepsilon)\prod_{j=0}^{n-2} R_j(\varepsilon) - 2^{2n-2}\left(\prod_{j=0}^{n-2} R_j(\varepsilon)\right)^2 \\ &= -2^{2n-2}\left(\prod_{j=0}^{n-2} R_j(\varepsilon)\right)^2 . \end{aligned} \tag{9}$$

From Lemma 1, $R_j(\varepsilon) \neq 0$ for $0 \leq j \leq n-2$. Thus $P_n(\varepsilon; a) < 0$. Clearly we have $P_n(0; a) = 1 > 0$, since $n \geq 2$. Therefore $P_n(X; a)$ has at least one real root which is between 0 and ε. Suppose θ is any root and let $\alpha = \theta + i$. Let $\beta = M\theta + i = \alpha(\varepsilon + i)/(\theta + \varepsilon)$. Note that $(\varepsilon + i)^{2^n} = R_n(\varepsilon) + iI_n(\varepsilon) = R_n(\varepsilon)$, since $R_{n-1}(X)$ divides $I_n(X)$. Since $(\varepsilon + i)^{2^n} \in \mathbb{R}$, we have

$$\begin{aligned} P_n(M\theta; a) &= \Re((M\theta + i)^{2^n}) - \frac{a}{2^n}\Im((M\theta + i)^{2^n}) \\ &= \left(\frac{\varepsilon + i}{\theta + \varepsilon}\right)^{2^n}\left(\Re(\alpha^{2^n}) - \frac{a}{2^n}\Im(\alpha^{2^n})\right) \\ &= \left(\frac{\varepsilon + i}{\theta + \varepsilon}\right)^{2^n} P_n(\theta; a) \\ &= 0. \end{aligned}$$

Therefore M permutes the roots. Since M has two distinct eigenvalues $\varepsilon + i$, $\varepsilon - i$, it must be similar to the diagonal matrix

$$D = \begin{pmatrix} \varepsilon + i & 0 \\ 0 & \varepsilon - i \end{pmatrix}.$$

Because the matrices M and D have the same order, it suffices to show that D is of order 2^n. Now for any z

$$Dz = \frac{\varepsilon + i}{\varepsilon - i} z = \zeta z,$$

where $\zeta = (\varepsilon + i)/(\varepsilon - i)$. Note that ε is real and $R_{n-1}(\varepsilon) = 0$. Therefore

$$(\varepsilon + i)^{2^{n-1}} = R_{n-1}(\varepsilon) + iI_{n-1}(\varepsilon) = iI_{n-1}(\varepsilon),$$

and hence

$$(\varepsilon - i)^{2^{n-1}} = \overline{(\varepsilon + i)}^{2^{n-1}} = -iI_{n-1}(\varepsilon).$$

Since $I_{n-1}(\varepsilon) \neq 0$ by Lemma 1, all these yield

$$\zeta^{2^{n-1}} = \left(\frac{\varepsilon + i}{\varepsilon - i}\right)^{2^{n-1}} = \frac{iI_{n-1}(\varepsilon)}{-iI_{n-1}(\varepsilon)} = -1,$$

and thus ζ is of order 2^n. But $Dz = \zeta z$, so the transformation D is of order 2^n and the only fixed points of a nontrivial power of D are 0 and ∞. It follows that i and $-i$ are the only fixed points of any nontrivial power of M. If θ is a root, the numbers $M^k\theta$, $0 \leq k < 2^n$, must be distinct roots of $P_n(X; a)$. This proves the theorem.

Remark. From the proof of the above theorem, we know that if ε is a root of $R_{n-1}(X)$ then the element $(\varepsilon + i)/(\varepsilon - i)$ is a primitive 2^nth root of unity. In fact, we have the following proposition:

Proposition 1. *The element* $(\varepsilon + i)/(\varepsilon - i)$ *is equal to*

$$\zeta_{2^n} = \exp\left(\frac{\pi i}{2^{n-1}}\right)$$

if ε *is the largest root of* $R_{n-1}(X)$.

Proof. Among the 2^{n-1} primitive 2^nth roots of unity, the roots

$$\zeta_{2^n} = \exp\left(\frac{\pi i}{2^{n-1}}\right) = \cos\left(\frac{\pi}{2^{n-1}}\right) + i\sin\left(\frac{\pi}{2^{n-1}}\right)$$

and $\zeta_{2^n}^{-1}$ have the largest real part. We have

$$\left\{\frac{\varepsilon + i}{\varepsilon - i}\middle| \varepsilon = \text{root of } R_{n-1}(X)\right\} = \left\{\exp\left(\frac{k\pi i}{2^{n-1}}\right)\middle| k = 1, 3, 5, \dots\right\}$$

(the left side is contained in the right side, and both have 2^{n-1} elements) and $\Re(\frac{\varepsilon+i}{\varepsilon-i}) = \frac{\varepsilon^2-1}{\varepsilon^2+1} = 1 - \frac{2}{\varepsilon^2+1}$ is the largest if ε is the largest root of $R_{n-1}(X)$. Also $\Im(\frac{\varepsilon+i}{\varepsilon-i}) = \frac{2\varepsilon}{\varepsilon^2+1} > 0$. This proves the proposition.

For each natural number n, we let ε_n be the largest root of the polynomial $R_n(X)$. We know that

$$\varepsilon_0 = 0, \quad \varepsilon_1 = 1, \quad \varepsilon_2 = 1 + \sqrt{2}.$$

How are these ε_n 's related? From the above proposition, we have

$$\frac{\varepsilon_{n-1} + i}{\varepsilon_{n-1} - i} = \zeta_{2^n},$$

where $\zeta_{2^n} = \exp(\pi i/2^{n-1})$. Solving this equation for ε_{n-1}, we get

$$\varepsilon_{n-1} = -i\frac{1 + \zeta_{2^n}}{1 - \zeta_{2^n}} = \cot\left(\frac{\pi}{2^n}\right).$$

Calculation shows $\varepsilon_n^2 - 2\varepsilon_{n-1}\varepsilon_n - 1 = 0$ and hence $\varepsilon_n = \varepsilon_{n-1} + \sqrt{\varepsilon_{n-1}^2 + 1}$. Note also $\varepsilon_{n-1} = \frac{1}{2}(\varepsilon_n - \frac{1}{\varepsilon_n})$, and we have proved the next proposition.

Proposition 2. *Let ε_n be the largest root of the polynomial $R_n(X)$. Then*

$$\varepsilon_n = -i\frac{1+\zeta_{2^{n+1}}}{1-\zeta_{2^{n+1}}} = \cot\left(\frac{\pi}{2^{n+1}}\right),$$

and hence the formula $\varepsilon_n = \varepsilon_{n-1} + \sqrt{\varepsilon_{n-1}^2 + 1}$, or $\varepsilon_{n-1} = \frac{1}{2}(\varepsilon_n - \frac{1}{\varepsilon_n})$.

As a matter of fact, the extension field $\mathbb{Q}(\varepsilon_n)$ is the real cyclotomic field $\mathbb{Q}(\zeta_{2^{n+1}})^+$. This is the content of the next proposition.

Proposition 3. *Let ε_n be any root of the polynomial $R_n(X)$. Then*

$$\mathbb{Q}(\varepsilon_n) = \mathbb{Q}(\zeta_{2^{n+1}})^+.$$

Proof. Since $(\varepsilon_n + i)/(\varepsilon_n - i) = \zeta$, for some primitive 2^{n+1}th root of unity ζ, we have $\varepsilon_n = -i(1+\zeta)/(1-\zeta)$. Let $\sigma\colon \zeta \mapsto \zeta^d$ be an automorphism of $\mathbb{Q}(\zeta)$ that fixes the element ε_n. Then

$$i^d\frac{1+\zeta^d}{1-\zeta^d} = i\frac{1+\zeta}{1-\zeta}.$$

Since d is odd, $i^d = \pm i$.

$$i^d = +i\colon (1+\zeta^d)(1-\zeta) = (1-\zeta^d)(1+\zeta) \Rightarrow \zeta^d = \zeta \Rightarrow \sigma = \mathrm{id}.$$
$$i^d = -i\colon (1+\zeta^d)(1-\zeta) = -(1-\zeta^d)(1+\zeta) \Rightarrow \zeta^{d+1} = 1 \Rightarrow \zeta^d = \zeta^{-1},$$

and hence $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^+)$. Since $i\frac{1+\zeta}{1-\zeta} \in \mathbb{Q}(\zeta)^+$ is only fixed by $\{\mathrm{id}, \sigma_{-1}\}$, the proposition is proved.

4. Irreducibility of the 2^n-tic polynomials

Theorem 2. *Let $a \in \mathbb{Z}$. The 2^n-tic polynomial $P_n(X; a)$ is irreducible over the rationals $\mathbb{Q}$ if and only if $a^2 + 4^n$ is not a square in rational integers.*

Remarks. (1) It is easy to see that $a^2 + 4^n = b^2$ has only $2n-1$ solutions for rational integers a. They are

$$a = \pm(2^{2k}-1)2^{n-k-1}, \qquad 0 \le k < n.$$

(2) The cases $n = 1, 2, 3$ were proved in [11, 4, 13], so in the following proof we may assume $n \ge 4$.

Proof. If $a^2 + 4^n$ is a square, then $P_n(X; a)$ factors, by (6). Conversely, if θ is a root of $P_n(X; a)$, then the 2^n roots are $\{M^j\theta | 0 \le j < 2^n\}$, where $M = \left(\begin{smallmatrix}\varepsilon & -1\\ 1 & \varepsilon\end{smallmatrix}\right)$ and $\frac{\varepsilon+i}{\varepsilon-i} = \zeta_{2^n}$. We know that $M = A^{-1}DA$, where $D = \left(\begin{smallmatrix}\varepsilon+i & 0\\ 0 & \varepsilon-i\end{smallmatrix}\right)$, and one choice for A is $\left(\begin{smallmatrix}1 & +i\\ 1 & -i\end{smallmatrix}\right)$. Therefore $M^j = A^{-1}D^jA$, and hence $AM^j = D^jA$. Let $\alpha = A\theta = \frac{\theta+i}{\theta-i}$. Then

$$\frac{M^j\theta + i}{M^j\theta - i} = AM^j\theta = D^jA\theta = D^j\alpha = \zeta_{2^n}^j\alpha.$$

Since $\varepsilon \in \mathbb{Q}(\zeta_{2^n})$, all the roots of $P_n(X; a)$ lie in $\mathbb{Q}(\theta, \zeta_{2^n})$, so it is Galois over $\mathbb{Q}(\zeta_{2^n})$. If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta, \zeta_{2^n})/\mathbb{Q}(\zeta_{2^n}))$, then $\sigma\theta = M^j\theta$ for some j. Let $\beta = \alpha^{2^n}$. By the above, $\sigma\alpha = \zeta_{2^n}^j\alpha$, so $\sigma\beta = \beta$. Therefore $\beta \in \mathbb{Q}(\zeta_{2^n})$, and we have the following.

$$\mathbb{Q}(\zeta_{2^n}, \theta) = \mathbb{Q}(\zeta_{2^n}, \sqrt[2^n]{\beta}) \text{ is of degree } 2^n \text{ over } \mathbb{Q}(\zeta_{2^n}) \Leftrightarrow \beta \notin \mathbb{Q}(\zeta_{2^n})^2.$$

Calculation shows $\beta \in \mathbb{Q}(i)$ as follows: (Note $P_n(\theta\,; a) = R_n(\theta) - \frac{a}{2^n} I_n(\theta) = 0$)

$$\beta = \alpha^{2^n} = \frac{(\theta + i)^{2^n}}{(\theta - i)^{2^n}} = \frac{R_n(\theta) + iI_n(\theta)}{R_n(\theta) - iI_n(\theta)} = \frac{a + i2^n}{a - i2^n} \in \mathbb{Q}(i).$$

Suppose $\sqrt{\beta} \in \mathbb{Q}(\zeta_{2^n})$. Since the cyclotomic field $\mathbb{Q}(\zeta_{2^n})$ is cyclic of degree 2^{n-2} over the field $\mathbb{Q}(i)$, the extension field $\mathbb{Q}(i)(\sqrt{\beta})$ is either $\mathbb{Q}(i)$ or the quadratic extension $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i)(\sqrt{2})$.

Case I. $\sqrt{\beta} \in \mathbb{Q}(i)$. Since $\beta = \frac{a+i2^n}{a-i2^n} = \frac{a^2+4^n}{(a-i2^n)^2}$, we have

$$a^2 + 4^n \in \mathbb{Q}(i)^2 \Rightarrow a^2 + 4^n = (x + iy)^2 = x^2 - y^2 + 2ixy$$
$$\Rightarrow xy = 0 \text{ and } x^2 - y^2 > 0 \Rightarrow y = 0 \Rightarrow a^2 + 4^n \in \mathbb{Q}^2.$$

We know that $P_n(X\,; a)$ factors over the rationals in this case.

Case II. $\mathbb{Q}(i)(\sqrt{\beta}) = \mathbb{Q}(i)(\sqrt{2})$. The element $\sqrt{\frac{\beta}{2}}$ is fixed by the Galois group $\mathrm{Gal}(\mathbb{Q}(i)(\sqrt{\beta})/\mathbb{Q}(i))$. Thus $\frac{\beta}{2}$ is a square in $\mathbb{Q}(i)$, and as above we have

$$a^2 + 4^n = 2(x + iy)^2 = 2(x^2 - y^2) + 4ixy \Rightarrow y = 0 \Rightarrow a^2 + 4^n \in 2\mathbb{Q}^2.$$

So far, we have shown that if $a^2 + 4^n \notin \mathbb{Q}^2$ or $2\mathbb{Q}^2$, then the extension field $\mathbb{Q}(\zeta_{2^n}, \alpha)$ is cyclic of degree 2^n over $\mathbb{Q}(\zeta_{2^n})$. Therefore, since $\mathbb{Q}(\zeta_{2^n}, \theta) = \mathbb{Q}(\zeta_{2^n}, \alpha)$, the field extension $\mathbb{Q}(\theta)/\mathbb{Q}$ has degree $\geq 2^n$, so the polynomial $P_n(X\,; a)$ is irreducible over the rationals.

It remains to show that if $a^2 + 4^n = 2x^2$ for some integer x then the polynomial $P_n(X\,; a)$ is also irreducible over the rationals. Equation (6) tells us that the polynomial $P_n(X\,; a)$ factors over the field $\mathbb{Q}(\sqrt{a^2 + 4^n}) = \mathbb{Q}(\sqrt{2})$. We will show that $P_{n-1}(X\,; \frac{a\pm\sqrt{a^2+4^n}}{2})$ is irreducible over the field $\mathbb{Q}(\sqrt{2})$, if β is not a 4th power in the field $\mathbb{Q}(\zeta_{2^n})$.

Consider the following diagram: ($N = [\mathbb{Q}(\zeta_{2^n})(\theta) : \mathbb{Q}(\zeta_{2^n})]$)

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{2^n})(\sqrt[2^n]{\beta}) \arrow[d, equal] & \\
 & \mathbb{Q}(\zeta_{2^n})(\theta) \arrow[dl, dash] \arrow[dr, dash, "N"] & \\
\mathbb{Q}(\theta)(\sqrt{2}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{2^n}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2}) &
\end{tikzcd}$$

If $\beta = \frac{a+2^n i}{a-2^n i} \neq$ 4th power in $\mathbb{Q}(\zeta_{2^n})$, then $N \geq 2^{n-1}$. Since $\mathbb{Q}(\theta)(\sqrt{2})/\mathbb{Q}(\sqrt{2})$ is generated by a root of $P_{n-1}(X\,; \frac{a\pm\sqrt{a^2+4^n}}{2})$, which is of degree 2^{n-1}, this polynomial (and its conjugate by $\sqrt{2} \mapsto -\sqrt{2}$) is irreducible over the field $\mathbb{Q}(\sqrt{2})$. Since $P_{n-1}(X\,; \frac{a\pm\sqrt{a^2+4^n}}{2}) \notin \mathbb{Q}[X]$, it follows easily that $P_n(X\,; a)$ is irreducible over the rationals.

Finally, we take care of the situation when the element $\beta = \frac{a+2^n i}{a-2^n i}$ is a 4th power in the field $\mathbb{Q}(\zeta_{2^n})$. This is done in the following lemma.

Lemma 2. *Let $a \in \mathbb{Z}$ and assume a^2+4^n is not a square in $\mathbb{Z}$. If the element $\beta = \frac{a+2^n i}{a-2^n i}$ is a 4th power in the field $\mathbb{Q}(\zeta_{2^n})$, then $a/2^n = \pm 1$ or ± 239.*

Proof. Assume $\sqrt[4]{\beta} \in \mathbb{Q}(\zeta_{2^n})$. Since $\mathbb{Q}(\zeta_{2^n})$ is cyclic of degree 2^{n-2} over the field $\mathbb{Q}(i)$, the field $\mathbb{Q}(i)(\sqrt[4]{\beta})$ is one of the following fields for $n \geq 4$,

$$\mathbb{Q}(i), \quad \mathbb{Q}(\zeta_8), \quad \mathbb{Q}(\zeta_{16}).$$

So we have $\beta = i^c \cdot \gamma^4$, where $c = 0, 1, 2, 3$, and $\gamma \in \mathbb{Q}(i)$.

(1) $c=0$: Letting $(a-2^n i)\gamma^2 = s+it$, we have

$$\frac{a+2^n i}{a-2^n i} = \gamma^4 \Rightarrow a^2+4^n = ((a-2^n i)\gamma^2)^2 = (s+it)^2 = s^2-t^2+2sti$$
$$\Rightarrow st = 0, \text{ and } s^2-t^2>0 \text{ since } a^2+4^n>0 \Rightarrow t=0 \Rightarrow a^2+4^n = s^2.$$

This contradicts our assumption.

(2) $c=2$: $\frac{a+2^n i}{a-2^n i} = -\gamma^4 \Rightarrow a^2+4^n = -(s+it)^2$, which is impossible, as in case (1).

(3) $c=1$: $\frac{a+2^n i}{a-2^n i} = i\gamma^4$. (See below.)

(4) $c=3$: $\frac{a+2^n i}{a-2^n i} = -i\gamma^4 \Rightarrow \frac{a-2^n i}{a+2^n i} = i\overline{\gamma}^4 \Rightarrow \frac{(-a)+2^n i}{(-a)-2^n i} = i\overline{\gamma}^4$, so we are in case (3) by taking the negative of a and the complex conjugate of γ.

For case (3), we have $a^2+4^n = i((a-2^n i)\gamma^2)^2 = i\gamma_1^2$, where $\gamma_1 = (a-2^n i)\gamma^2$. Write $\gamma_1 = s+it$, for $s, t \in \mathbb{Q}$. Then we have

$$i\gamma_1^2 = i(s^2-t^2)-2st = a^2+4^n \Rightarrow s^2=t^2 \Rightarrow t=\pm s, \quad -2st>0 \Rightarrow t=-s.$$

Therefore $2s^2 = a^2+4^n$ and $\gamma_1 = s(1-i)$, and hence $(a-2^n i)\gamma^2 = s(1-i)$. Write $\gamma = \frac{u+vi}{w}$ with $u, v \in \mathbb{Z}$, $w \in \mathbb{Q}$, $(u, v)=1$. Since $N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta) = 1$, the same holds for γ, so $u^2+v^2=w^2$, hence $w \in \mathbb{Z}$ and $u \not\equiv v \bmod 2$. We have

$$(a-2^n i)(u^2-v^2+2uvi) = sw^2(1-i),$$

and therefore the identities

$$a(u^2-v^2)+2^{n+1}uv = sw^2, \text{ and } \quad 2uva-2^n(u^2-v^2) = -sw^2. \tag{10}$$

Putting them together and solving for a, we get

$$a = \frac{2^n(u^2-v^2-2uv)}{u^2-v^2+2uv} = \frac{2^n}{\delta}(\delta-4uv), \tag{11}$$

where $\delta = u^2-v^2+2uv$.

Claim. $\delta = \pm 1$.

Proof of the Claim. Since $u \not\equiv v \bmod 2$, we have $\delta \equiv 1 \bmod 2$. Suppose p is an odd prime such that $p \mid \delta$. Since $a \in \mathbb{Z}, p \mid (\delta-4uv)$, and so $p \mid 4uv$. Therefore $p \mid u$ or $p \mid v$. If $p \mid u$ then $p \mid v^2$, and if $p \mid v$ then $p \mid u^2$. Both contradict $(u, v)=1$. So $\delta = \pm 1$. This completes the proof of the claim.

A straightforward calculation, eliminating a from the two equations in (11), yields $sw^2\delta = 2^n(u^2+v^2)^2 = 2^n w^4$, so $s\delta = 2^n w^2$. From (11), we have $a = 2^n y$, with $y = 1-4\delta uv$, hence $2^{2n+1}w^4 = 2s^2 = 4^n(y^2+1)$. This implies that $2w^4 = y^2+1$, $w, y \in \mathbb{Z}$. The integral solutions of this Diophantine equation are [9, 14] $y=\pm 1$, $w=\pm 1$, and $y=\pm 239$, $w=\pm 13$.

First Solution. Case (3) gives us $a = 2^n$ since

$$y = \pm 1 \Rightarrow 1 - 4\delta uv = \pm 1 \Rightarrow 4\delta uv = 0 \Rightarrow a = 2^n.$$

Similarly, case (4) yields $a = -2^n$. For these two a's, we have

$$\frac{a + 2^n i}{a - 2^n i} = \frac{\pm 2^n + 2^n i}{\pm 2^n - 2^n i} = \pm i,$$

and therefore

$$\left(\frac{\theta + i}{\theta - i}\right)^{2^n} = \pm i \Rightarrow \frac{\theta + i}{\theta - i} = \zeta_{2^{n+2}},$$

which yields

$$\theta = -i \frac{1 + \zeta_{2^{n+2}}}{1 - \zeta_{2^{n+2}}}.$$

From Proposition 3, we have $\mathbb{Q}(\theta) = \mathbb{Q}(\zeta_{2^{n+2}})^+$. Therefore we have

$$\deg(\mathbb{Q}(\theta)/\mathbb{Q}) = \frac{1}{2}\phi(2^{n+2}) = 2^n,$$

and sc $P_n(X; a)$ is irreducible for $a = \pm 2^n$.

Second Solution. Case (3) gives us $a = -239 \cdot 2^n$ since

$$y = \pm 239 \Rightarrow 1 - 4\delta uv = \pm 239 \Rightarrow 4\delta uv = 240 \Rightarrow a = -239 \cdot 2^n.$$

Similarly, case (4) yields $a = 239 \cdot 2^n$.

Lemma 3. *The polynomials* $P_n(X; \pm 239 \cdot 2^n)$ *are irreducible over* $\mathbb{Q}$.

Proof. Applying formula (6) twice, we get

$$P_n(X; \pm 239{\cdot}2^n) = P_{n-2}(X; 2^n\alpha_1)P_{n-2}(X; 2^n\alpha_2)P_{n-2}(X; 2^n\alpha_3)P_{n-2}(X; 2^n\alpha_4);$$

where

$$\begin{aligned}
\alpha_1 &= \pm 239 + 169\sqrt{2} + 13(7 \pm 5\sqrt{2})\sqrt{4 \pm 2\sqrt{2}}, \\
\alpha_2 &= \pm 239 + 169\sqrt{2} - 13(7 \pm 5\sqrt{2})\sqrt{4 \pm 2\sqrt{2}}, \\
\alpha_3 &= \pm 239 - 169\sqrt{2} + 13(7 \mp 5\sqrt{2})\sqrt{4 \mp 2\sqrt{2}}, \\
\alpha_4 &= \pm 239 - 169\sqrt{2} - 13(7 \mp 5\sqrt{2})\sqrt{4 \mp 2\sqrt{2}}.
\end{aligned}$$

Note that

$$P_{n-2}(X; 2^n\alpha_i)P_{n-2}(X; 2^n\alpha_j) = X^{2^{n-1}} - 2^{n-2}(\alpha_i + \alpha_j)X^{2^{n-1}-1} + \cdots,$$

and $\alpha_i + \alpha_j \notin \mathbb{Q}$, $\forall i, j$. This can be seen by using the fact that $\{1, \sqrt{4 + 2\sqrt{2}}\}$ is linearly independent over $\mathbb{Q}(\sqrt{2})$ and $\sqrt{4 - 2\sqrt{2}} = (\sqrt{2} - 1)\sqrt{4 + 2\sqrt{2}}$. Therefore none of the factors $P_{n-2}(X; 2^n\alpha_i)$ or products of two of them are in $\mathbb{Q}[X]$. Since

$$\mathbb{Q}(\zeta_{16})^+ = \mathbb{Q}(\sqrt{4 + 2\sqrt{2}}) = \mathbb{Q}(\sqrt{4 - 2\sqrt{2}}),$$

these polynomials are in $\mathbb{Q}(\zeta_{16})^+[X]$.

We will show below that each $P_{n-2}(X; 2^n\alpha_i)$ is irreducible in $\mathbb{Q}(\zeta_{16})^+[X]$. It then follows that $P_n(X; \pm 239 \cdot 2^n)$ is irreducible in $\mathbb{Q}[X]$.

Observe that

$$\frac{\pm 239\cdot 2^n + 2^n i}{\pm 239\cdot 2^n - 2^n i} = \frac{\pm 239 + i}{\pm 239 - i} = \mp i\left(\frac{5\mp 12i}{13}\right)^4 .$$

Suppose $\mp i(\frac{5\mp 12i}{13})^4$ is an 8th power in $\mathbb{Q}(\zeta_{2^m})$. We may assume $m \geq 5$, so $\pm i$ is an 8th power. Therefore $\frac{5\mp 12i}{13}$ is a square, say x^2, with $x \in \mathbb{Q}(\zeta_{2^m})$. Since $x^2 \in \mathbb{Q}(i)$, we have $\mathbb{Q}(i)(x) = \mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_8)$. This implies that

$$\frac{5\mp 12i}{13} \text{ is a square or } i(\text{square}) \text{ in } \mathbb{Q}(i).$$

Since $5\mp 12i = (3\mp 2i)^2$, 13 is a square or i(square) in $\mathbb{Q}(i)$, which is impossible. Therefore $\mp i(\frac{5\mp 12i}{13})^4$ is not an 8th power in $\mathbb{Q}(\zeta_{2^n})$, and hence the field extension $\mathbb{Q}(\zeta_{2^n}, \sqrt[2^n]{\mp i(\frac{5\mp 12i}{13})^4})$ over $\mathbb{Q}(\zeta_{2^n})$ has degree $\geq 2^{n-2}$.

$$\begin{tikzcd}
& \mathbb{Q}\left(\zeta_{2^n}, \sqrt[2^n]{\mp i\left(\frac{5\mp 12i}{13}\right)^4}\right) \arrow[dl, dash] \arrow[dr, dash, "\geq 2^{n-2}"] & \\
\mathbb{Q}(\sqrt{4+2\sqrt{2}})(\theta) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{2^n}) \arrow[dl, dash] \\
& \mathbb{Q}(\sqrt{4+2\sqrt{2}}) &
\end{tikzcd}$$

This gives us that

$$[\mathbb{Q}(\sqrt{2+\sqrt{2}})(\theta) : \mathbb{Q}(\sqrt{2+\sqrt{2}})] \geq 2^{n-2}.$$

Since θ is a root of some $P_{n-2}(X\,;\, 2^n\alpha_i)$, this polynomial and its conjugates over $\mathbb{Q}$ must be irreducible in $\mathbb{Q}(\zeta_{16})^+[X]$. This completes the proof of the lemma, and hence the proof of the irreducibility criterion for $P_n(X\,;\,a)$.

5. Units and roots of the 2^n-tic Polynomial

In this section, we assume $a^2 + 4^n$ is not a square in the rationals so that $P_n(X\,;\,a)$ is irreducible in $\mathbb{Z}[X]$. Moreover, for simplicity we assume that $a^2 + 4^n \neq 2s^2$, $s \in \mathbb{Z}$. As in the proof of Theorem 2, this implies that $P_n(X\,;\,a)$ is irreducible over $\mathbb{Q}(\zeta_{2^n})$. Fix a root θ of $P_n(X\,;\,a)$, so the roots are of the form $M^k\theta$, $0 \leq k < 2^n$, where $M = \left(\begin{smallmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{smallmatrix}\right)$ and $\varepsilon = -i\frac{1+\zeta_{2^n}}{1-\zeta_{2^n}} = \cot(\frac{\pi}{2^n})$. Let

$$K = \mathbb{Q}(\varepsilon) = \mathbb{Q}(\zeta_{2^n})^+.$$

Then it is easy to see that $K(\theta)$ is the Galois closure of $\mathbb{Q}(\theta)$. The above assumptions on a imply that $\mathrm{Gal}(K(\theta)/K) = \langle\tau\rangle$ is cyclic of order 2^n, where

$$\tau\colon \theta \mapsto \frac{\varepsilon\theta - 1}{\theta + \varepsilon}.$$

Note that we have

$$\tau^k(\theta) = M^k\theta, \qquad 0 \leq k < 2^n.$$

Since the constant term of $P_n(X; a)$ is 1 (if $n \geq 2$), these $\tau^k(\theta)$ are units in the ring of integers of $K(\theta)$. Obviously, these 2^n units are not independent, for instance, $\tau^{2^{n-1}}(\theta) = -\frac{1}{\theta}$. However, one half of them, say the first half

$$\{\tau^{k-1}(\theta) | 1 \leq k \leq 2^{n-1}\},$$

are independent. We prove this in the next theorem.

Theorem 3. *The* 2^{n-1} *elements*

$$\{\tau^{k-1}(\theta) | 1 \leq k \leq 2^{n-1}\}$$

are independent units in the ring $\mathcal{O}_{K(\theta)}$ *of integers of the field* $K(\theta)$, *where* $K = \mathbb{Q}(\varepsilon) = \mathbb{Q}(\zeta_{2^n})^+$.

Proof. Let $m = 2^{n-1}$ and let $\theta_k = \tau^{k-1}(\theta)$, $1 \leq k \leq m$. Then

$$\theta_{k+m} = \tau^m(\theta_k) = -\frac{1}{\theta_k}, \qquad \text{for } 1 \leq k \leq m. \tag{12}$$

Suppose we have $b_1, b_2, b_3, \dots, b_m \in \mathbb{Z}$ such that

$$\theta_1^{b_1}\theta_2^{b_2}\theta_3^{b_3}\cdots\theta_m^{b_m} = 1. \tag{13}$$

Apply $\tau, \dots, \tau^{m-1}$ to (13) and use formula (12), we get

$$\begin{aligned} (-\tfrac{1}{\theta_1})^{b_m}\theta_2^{b_1}\theta_3^{b_2}\cdots\theta_{m-1}^{b_{m-2}}\theta_m^{b_{m-1}} &= 1, \\ (-\tfrac{1}{\theta_1})^{b_{m-1}}(-\tfrac{1}{\theta_2})^{b_m}\theta_3^{b_1}\cdots\theta_{m-1}^{b_{m-3}}\theta_m^{b_{m-2}} &= 1, \\ \vdots \qquad\qquad & \;\vdots\;\; \vdots \\ (-\tfrac{1}{\theta_1})^{b_2}(-\tfrac{1}{\theta_2})^{b_3}\cdots(-\tfrac{1}{\theta_{m-1}})^{b_m}\theta_m^{b_1} &= 1. \end{aligned}$$

Take absolute values and then take logarithms of the above m equations. Write this system in matrix form as follows:

$$\begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_{m-1} & b_m \\ -b_m & b_1 & b_2 & \cdots & b_{m-2} & b_{m-1} \\ -b_{m-1} & -b_m & b_1 & \cdots & b_{m-3} & b_{m-2} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ -b_2 & -b_3 & -b_4 & \cdots & -b_m & b_1 \end{pmatrix} \begin{pmatrix} \log|\theta_1| \\ \log|\theta_2| \\ \log|\theta_3| \\ \vdots \\ \log|\theta_m| \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

If B is the coefficient matrix, then $\det(B) = 0$.

Lemma 4. $\det(B) = \prod_{\zeta^m=-1} \sum_{k=1}^m b_k \zeta^{k-1}$.

Proof. Let ζ be any primitive $2m$th root of unity, so $\zeta^m = -1$. Then

$$\begin{pmatrix} 1 \\ \zeta \\ \vdots \\ \zeta^{m-1} \end{pmatrix}$$

is an eigenvector of B with eigenvalue $\sum_{k=1}^m b_k \zeta^{k-1}$. Since ζ can take on m different values, we have a full set of eigenvectors. The determinant is the product of the eigenvalues.

By the lemma, we have $\sum_{k=1}^m b_k \zeta^{k-1} = 0$, for some primitive $2m$th root of unity ζ. Since $\phi(2m) = m$, the set $\{1, \zeta, \dots, \zeta^{m-1}\}$ is linearly independent over the rationals, and hence $b_1 = b_2 = \cdots = b_m = 0$. Therefore the 2^n units $\{\tau^{k-1}(\theta) | 1 \leq k \leq 2^{n-1}\}$ are independent. This completes the proof of the theorem.

So far we have 2^{n-1} independent units, all of which are roots of $P_n(X; a)$. If the field $\mathbb{Q}(\theta)$ is Galois over the rationals, then the rank of the unit group is $2^n - 1$ and we need $2^{n-1} - 1$ more units in order to get a set of units which is close to being a system of fundamental units. This is the case when $n \leq 2$ or when $n = 3$ for a selected family of a's. Unfortunately, the field $\mathbb{Q}(\theta)$ is not Galois over the rationals in general. We know that $K(\theta)$ is the Galois closure of $\mathbb{Q}(\theta)$ so that the rank of the unit group is $4^{n-1} - 1$ and we need many more units to reach the same goal. Although the set of the cyclotomic units in $K = \mathbb{Q}(\zeta_{2^n})^+ = \mathbb{Q}(\varepsilon)$ will be part of them, it does not help us enough. In the next section we show how to obtain additional units from subfields of $K(\theta)$, though we still do not obtain a maximal set of independent units.

6. A SET OF $2^n - 1$ INDEPENDENT UNITS

Define a sequence (u_j) of real numbers as follows:

$$u_0 = \theta \quad \text{and} \quad u_j = \frac{1}{2}\left(u_{j-1} - \frac{1}{u_{j-1}}\right), \quad \text{for } 1 \leq j \leq n.$$

For convenience, we denote the field $\mathbb{Q}(u_j)$ by K_j for $1 \leq j \leq n$. Obviously, we have the following lemma.

Lemma 5. *The element u_{j-1} satisfies the quadratic polynomial*

$$P_1(X; 2u_j) = X^2 - 2u_jX - 1, \quad \textit{for } 1 \leq j \leq n;$$

and hence the degree $\deg(K_{j-1}/K_j)$ of u_{j-1} over the field K_j is 1 or 2.

Lemma 6. *We have the following identities:*

$$u_{m+j} = \frac{R_j(u_m)}{I_j(u_m)}, \quad \textit{for } 0 \leq m + j \leq n.$$

In particular, $u_n = \frac{a}{2^n}$, and therefore $K_n = \mathbb{Q}$.

Proof. From (1) and (2), we have, for $j = 1, 2, 3, \ldots, n$

$$\frac{R_j(X)}{I_j(X)} = \frac{1}{2}\left(\frac{R_{j-1}(X)}{I_{j-1}(X)} - \frac{I_{j-1}(X)}{R_{j-1}(X)}\right). \tag{14}$$

For $j = 0$ the lemma is trivial, since $R_0(X)/I_0(X) = X$. Assuming it is true for $j - 1$, we easily find from (14) that it is true for j. Letting $j = n$ in the lemma, and using the fact that $P_n(\theta; a) = 0$, we find that

$$u_n = \frac{R_n(\theta)}{I_n(\theta)} = \frac{a}{2^n}.$$

Therefore $K_n = \mathbb{Q}$. This completes the proof of the lemma.

Proposition 4. *For $a \neq \pm(2^{2k} - 1)2^{n-k-1}$, $0 \leq k < n$; the degree of the element u_{j-1} over the field K_j is 2, for $1 \leq j \leq n$.*

Proof. We have

$$\deg(\mathbb{Q}(\theta)/\mathbb{Q}) = \deg(K_0/K_1)\deg(K_1/K_2)\deg(K_2/K_3)\cdots\deg(K_{n-1}/K_n).$$

The irreducibility of $P_n(X; a)$ gives us $\deg(\mathbb{Q}(\theta)/\mathbb{Q}) = 2^n$, and so the degree $\deg(K_{j-1}/K_j)$ of the element u_{j-1} over the field K_j is 2, for $1 \leq j \leq n$. This completes the proof of the proposition.

Theorem 4. *The element u_j satisfies the polynomial*

$$P_{n-j}(X; a/2^j), \quad \textit{for } 1 \leq j \leq n.$$

Furthermore, the field K_j is a simplest 2^{n-j}-tic field over the rationals, if 2^j divides a. In this case, the element u_j is also a unit in the ring $\mathscr{O}_{K(\theta)}$ of integers of $K(\theta)$.

Proof. Lemma 6 tells us that the element u_j satisfies the polynomial

$$R_{n-j}(X) - \frac{a}{2^n} I_{n-j}(X),$$

which is in fact the polynomial

$$R_{n-j}(X) - \frac{a/2^j}{2^{n-j}} I_{n-j}(X) = P_{n-j}\left(X; \frac{a}{2^j}\right).$$

This completes the proof of the theorem.

Remark. More generally, we see that u_m is a root of $P_j(X; 2^j u_{m+j})$, so each intermediate extension K_m/K_{m+j} could be regarded as being "of simplest type."

From the previous theorem, we have for each $0 \leq j < n$ that the element u_j is a unit in the ring $\mathscr{O}_{K(\theta)}$ if 2^j divides a. Theorem 3 gives us 2^{n-j-1} independent units, namely

$$\{\tau^{2^j(k-1)}(u_j) | 1 \leq k \leq 2^{n-j-1}\}$$

in the ring $\mathscr{O}_{K(u_j)}$ of integers of the field $K(u_j)$. Putting all these units together, we have in total

$$2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2^1 + 2^0 = 2^n - 1$$

units in the field $K(\theta)$. Are these units independent? The answer is yes, and we will prove this in the following theorem.

Theorem 5. *Let $a \in \mathbb{Z}$ and let $2^n | a$. Then the $2^n - 1$ elements*

$$\{\tau^{2^j(k-1)}(u_j) | 1 \leq k \leq 2^{n-j-1} \textit{ and } 0 \leq j < n\}$$

are independent units in the ring $\mathscr{O}_{K(\theta)}$ of algebraic integers of the field $K(\theta)$, where $K = \mathbb{Q}(\varepsilon) = \mathbb{Q}(\zeta_{2^n})^+$.

Proof. We will prove the theorem by induction on n. The result is trivial for $n = 1$. Assume the theorem is true for $n - 1$. Suppose we have rational integers $b_{k,j}$ such that

$$(15) \qquad \eta = \prod_{k=1}^{2^{n-1}} (\tau^{k-1}(u_0))^{b_{k,0}} = \prod_{j=1}^{n-1} \prod_{k=1}^{2^{n-j-1}} (\tau^{2^j(k-1)}(u_j))^{b_{k,j}} \in K(u_1).$$

Since the field $K(u_1)$ is fixed by the automorphism $\tau^{2^{n-1}}$, the element η is invariant under $\tau^{2^{n-1}}$. Note that $\tau^{2^{n-1}}(u_0) = -u_0^{-1}$, and so we have

$$\prod_{k=1}^{2^{n-1}} (\tau^{k-1}(u_0))^{b_{k,0}} = \eta = \tau^{2^{n-1}}(\eta) = \pm \prod_{k=1}^{2^{n-1}} (\tau^{k-1}(u_0))^{-b_{k,0}}.$$

Therefore, we have

$$\pm 1 = \prod_{k=1}^{2^{n-1}} (\tau^{k-1}(u_0))^{2b_{k,0}}.$$

Since the right-hand side is the square of a real number, we get

$$\prod_{k=1}^{2^{n-1}} (\tau^{k-1}(u_0))^{2b_{k,0}} = 1.$$

Theorem 3 tells us that $2b_{k,0} = 0$, $\forall k$; and hence $b_{k,0} = 0$, $\forall k$. Now, the relation in (15) becomes

$$\prod_{j=1}^{n-1} \prod_{k=1}^{2^{n-j-1}} (\tau^{2^j(k-1)}(u_j))^{b_{k,j}} = 1.$$

From the induction hypothesis, the $2^{n-1} - 1$ units

$$\{\tau^{2^j(k-1)}(u_j) | 1 \le k \le 2^{n-j-1} \text{ and } 1 \le j < n\}$$

are independent, and so $b_{k,j} = 0$, for $1 \le k \le 2^{n-j-1}$ and $1 \le j < n$. Therefore all $b_{k,j}$ are 0, and this completes the proof of the theorem.

Finally, we prove that the group Σ generated by these $2^n - 1$ independent units in the ring $\mathscr{O}_{K(\theta)}$ is almost fundamental in the sense that if $E_1 \supseteq \Sigma$ is a subgroup of the full unit group and $[E_1 : \Sigma]$ is finite, then this index is bounded uniformly as the parameter for the family varies, under certain mild restrictions. First, we have the following:

Theorem 6. *Fix* $n \ge 1$. *Let* $S = \langle \pm\theta_i ; 1 \le i \le 2^{n-1} \rangle$, *where* $\theta_i = \tau^{i-1}(\theta)$. *Let*

$$D = \{u \in \mathbb{Q}(\{\theta_1, \theta_2, \dots\}) | u^l \in S \textit{ for some } l \ne 0\}.$$

Let a run through a sequence of integers such that $(a^2 + 4^n)/\operatorname{osf}(a^2 + 4^n)$ *is bounded above, where* $\operatorname{osf}(x)$ *is the odd squarefree part of an integer* x (*so* $x = \operatorname{osf}(x)$ *times a square times a power of* 2). *Then the index* $[D : S]$ *is bounded independently of* a.

Remark. This result says that the units S form an "almost fundamental piece" of the unit group, in the sense that it is only necessary to enlarge S by a bounded amount in order to obtain a direct summand of the full unit group. In the corollary below, we obtain a similar result for the group Σ generated by the units of Theorem 5.

Proof. By taking a large enough, we may assume that $a^2 + 4^n$ is neither a square nor twice a square. Therefore, as in the proof of Theorem 2, $K(\theta)/K$ has degree 2^n. Let $\widetilde{S} = S/\{\pm 1\}$ and $\widetilde{D} = D/\{\pm 1\}$. Let $d \in D$ and let $d^l \in S$. Then $\tau^{2^{n-1}}(d^l) = \pm d^{-l}$. Since d and $\tau^{2^{n-1}}(d)$ are real, $(1 + \tau^{2^{n-1}})(d) = \pm 1$. Therefore $\mathbb{Z}[\tau]/(1 + \tau^{2^{n-1}}) \simeq \mathbb{Z}[\zeta_{2^n}]$ acts on $\widetilde{D}$, which we shall mostly write additively. If $0 \ne \alpha \in \mathbb{Z}[\zeta_{2^n}]$ and $d \in \widetilde{D}$ satisfy $\alpha d = 0$, then $(\operatorname{Norm} \alpha) d = 0$, which implies $d = 0$ since $\widetilde{D}$ is a torsion-free abelian group. Therefore $\widetilde{D}$ is a torsion-free $\mathbb{Z}[\zeta_{2^n}]$ module. Since it has $\mathbb{Z}$-rank 2^{n-1}, it must be isomorphic to an ideal of $\mathbb{Z}[\zeta_{2^n}]$ that is determined up to ideal class. Let $I_1, \dots, I_h$ be representatives for the ideal classes of $\mathbb{Q}(\zeta_{2^n})$. For each I_i, choose a principal ideal $0 \neq J_i \subseteq I_i$. Since $\widetilde{D} \simeq I_i$ for some i, we find that $\widetilde{D}$ has a cyclic submodule $\simeq J_i$ of finite index, with a bound on this index depending only on n. Let $\widetilde{C} = \mathbb{Z}[\zeta_{2^n}]\varepsilon_1 \subseteq \widetilde{D}$ be this submodule, where $\varepsilon_1 \in D$.

Let $\varepsilon_k = \tau^{k-1}(\varepsilon_1)$, $1 \leq k \leq 2^n$. Choose $l > 0$ such that

$$\varepsilon_1^l = \pm \prod_{i=1}^{2^{n-1}} \theta_i^{b_i}.$$

Then $\varepsilon_k^l = \pm \prod_{i=1}^{2^{n-1}} \theta_{i+k-1}^{b_i}$. Let $g\colon K \to \mathbb{R}$ be any embedding and extend g to $K(\theta)$ so that $g(\theta) = \theta_0 =$ largest root of $P_n(X; a)$. This is possible since $[K(\theta) : K] = \deg P_n$, so $g(\theta)$ can be chosen to be any root in $\mathbb{R}$ of P_n.

Let $\eta = \prod_{k=1}^{2^{n-1}} \varepsilon_k^{a_k}$, where the $a_k \in \mathbb{Z}$ are to be chosen later. Let $\eta_i = \tau^{i-1}(\eta)$, $1 \leq i \leq 2^n$. Since ε_k, $1 \leq k \leq 2^{n-1}$, are independent, and $\tau^{2^{n-1}}$ acts by inversion (modulo $\{\pm 1\}$), it follows that the η_i are distinct if some $a_k \neq 0$.

Under any embedding g as above, we have

$$0 \neq \prod_{1 \leq i < j \leq 2^n} (\eta_i - \eta_j)^2 = \prod_{|\eta_j| \leq |\eta_i|} \left(1 - \frac{\eta_j}{\eta_i}\right)^2 \prod_{k=1}^{2^{n-1}} \eta_k^{2m_k},$$

where $m_k \in \mathbb{Z}$ is bounded in terms of n. Since $\eta_{k+2^{n-1}} = \pm 1/\eta_k$, we have restricted the last product to $k \leq 2^{n-1}$. Note that each factor in the first product on the right is bounded by 2. We now obtain

$$\log \prod (\eta_i - \eta_j)^2 \leq A + B \sum_{k=1}^{2^{n-1}} |\log|\eta_k||$$

with A and B depending only on n, and independent of η and the embedding g.

There are 2^{n-2} embeddings $g\colon K \to \mathbb{R}$, and we regard each one extended to $K(\theta)$ as above. Then

$$\begin{aligned} \log \prod_g g\left(\prod (\eta_i - \eta_j)^2\right) &\leq 2^{n-2} A + B \sum_g \sum_{k=1}^{2^{n-1}} |\log|g\eta_k|| \\ &\leq A_1 + B_1 \left(\sum_g \sum_{k=1}^{2^{n-1}} \log^2 |g\eta_k| \right)^{1/2}, \end{aligned}$$

by Cauchy-Schwarz.

Let $L_k^g = \log|g\varepsilon_k|$, $1 \leq k \leq 2^n$. Note that $L_{k+2^{n-1}}^g = -L_k^g$. Since $\eta_k = \prod_{j=1}^{2^{n-1}} \varepsilon_{j+k-1}^{a_j}$, the last sum above becomes

$$\sum_g \sum_k \left(\sum_{j=1}^{2^{n-1}} a_j L_{j+k-1}^g \right)^2 = \sum_g (a_1, \dots, a_{2^{n-1}})(L^g)^2(a_1, \dots, a_{2^{n-1}})^t,$$

where L^g is the symmetric matrix $(L_{j+k-1}^g)_{1 \leq j, k \leq 2^{n-1}}$.

Let $S_i^g = \log|g\theta_i|$. Then $lL_k^g = \sum_{i=1}^{2^{n-1}} b_i S_{i+k-1}^g$. Define $b_{i+2^{n-1}} = -b_i$ for $1 \leq i \leq 2^{n-1}$, and regard the indices $\bmod 2^n$. Let $B = (b_{ij})$, where

$b_{ij} = b_{j-i+1}$. Let $S^g = (S^g_{i+j-1})_{1\le i,j\le 2^{n-1}}$. The above becomes $L^g = \frac{1}{l}BS^g$. Note that L^g and S^g are symmetric, so

$$(L^g)^2 = (L_g)(L_g)^t = \left(\frac{1}{l}B\right)(S^g)^2\left(\frac{1}{l}B\right)^t.$$

Our sum therefore equals

$$(a_1, \dots, a_{2^{n-1}})\left(\frac{1}{l}B\right)\left(\sum_g (S^g)^2\right)(a_1, \dots, a_{2^{n-1}})\left(\frac{1}{l}B\right)^t.$$

Lemma 7. *Let* $M = \left(\begin{smallmatrix}\varepsilon & -1\\ 1 & -\varepsilon\end{smallmatrix}\right)$. *As* g *runs through the* 2^{n-2} *embeddings* $K \to \mathbb{R}$, *the elements* $gM \in \mathrm{PGL}_2(\mathbb{R})$ *run through the powers*

$$M_0^u = \begin{pmatrix}\cot(\pi/2^n) & -1\\ 1 & -\cot(\pi/2^n)\end{pmatrix}^u, \qquad 0 < u < 2^n,\ u \equiv 1 \pmod 4).$$

Proof. After fixing one embedding such that M maps to M_0, we can regard the embeddings g as corresponding to elements of $\mathrm{Gal}(K/\mathbb{Q})$. Extend g to $\mathbb{Q}(\zeta_{2^n})$ such that $g(i) = i$. Then $g = \sigma_k$ with $k \equiv 1 \pmod 4$, where $\sigma_k(\zeta_{2^n}) = \zeta_{2^n}^k$. Since

$$M_0 = (\varepsilon - i)\begin{pmatrix}1 & 1\\ -i & i\end{pmatrix}\begin{pmatrix}\zeta_{2^n} & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ -i & i\end{pmatrix}^{-1}$$

(we have used the fact that $\zeta_{2^n} = (\varepsilon + i)/(\varepsilon - i)$), it follows that gM_0 and M_0^k differ by a scalar matrix. The lemma follows easily.

Let g_u correspond to the power u. Then $g_u(\theta_i) = g_u(M^{i-1}\theta) = M_0^{u(i-1)}\theta_0$. Thus

$$S_i^{g_u} = \log|M_0^{u(i-1)}\theta_0| = S_{u(i-1)},$$

where $S_k = S_k^{g_1}$ and the subscripts are taken $\bmod 2^n$.

Lemma 8. $\sum_g (S^g)^2 = sI$, *where* $s = 2^{n-2}\sum_{k=1}^{2^{n-1}} \log^2|M_0^k\theta_0|$.

Proof. Fix two indices $a \ne b$, $1 \le a, b \le 2^{n-1}$. The (a, b) entry in $\sum_g (S^g)^2$ is

$$\sum_u \sum_{i=1}^{2^{n-1}} S_{u(a+i-1)}S_{u(b+i-1)}.$$

Since $S_{u(a+i-1)}$ changes sign when i is changed to $i + 2^{n-1}$, the product of the two S's depends only on $i \bmod 2^{n-1}$. Since u is odd, we can change variables to obtain

$$\sum_u \sum_{k \bmod 2^{n-1}} S_kS_{k+(b-a)u}.$$

Let $2^v \| (b-a)$. Clearly $0 \le v \le n-2$ (we henceforth ignore the easy case $n = 1$). First assume $v \le n-3$. Given u, let $u_j = u + j2^{n-1-v}$ for $0 \le j < 2^{v+1}$ (so $u_j \equiv 1 \pmod 4$). Then

$$\begin{aligned} k + (b-a)u_j &\equiv k + (b-a)u + (b-a)j2^{n-1-v}\\ &\equiv k + (b-a)u + j2^{n-1} \pmod{2^n}. \end{aligned}$$

Therefore $S_kS_{k+(b-a)u_j} = (-1)^jS_kS_{k+(b-a)u}$, so $\sum_{i=0}^{2^{v+1}-1} S_kS_{k+(b-a)u_j} = 0$. Since the full sum is a sum of such sums, it must vanish.

If $v = n-2$, an easy calculation shows that the terms for k and $k+2^{n-2}$ cancel, so again the sum is zero.

If $a = b$, then the (a, a) entry is

$$2^{n-2}\sum_k S_k^2 = 2^{n-2}\sum_{k=1}^{2^{n-1}} \log^2 |M_0^k\theta_0| = s.$$

This proves the lemma.

Lemma 9. $s = O(\log^2|a|)$, *where the implied constant depends only on* n.

Proof. It is easy to show that the largest root θ_0 of $P_n(X; a)$ satisfies $\theta_0 = O(|a|)$, so $\log|\theta_0| = O(\log|a|)$. Therefore for $\pm 1/\theta_0$, the smallest root in absolute value, we have $\log|\pm 1/\theta_0| = O(\log|a|)$. Since the numbers $M_0^k\theta_0$ in the definition of s are the roots of $P_n(X; a)$, the lemma follows easily.

Consider the quadratic form

$$Q(a_1, \dots, a_{2^{n-1}}) = (a_1, \dots, a_{2^{n-1}})\left(\frac{1}{l}B\right) sI \left(\frac{1}{l}B\right)^t (a_1, \dots, a_{2^{n-1}})^t.$$

A theorem of Hermite (see Cassels [1, p. 31]) implies that there exists $0 \neq (a_1, \dots, a_{2^{n-1}}) \in \mathbb{Z}^{2^{n-1}}$ such that $Q(a_1, \dots, a_{2^{n-1}}) \leq \gamma(\det Q)^{1/2^{n-1}}$, where γ is the Hermite constant, which depends only on n. We choose η above corresponding to such a choice of a_k's. Since $\det Q = s^{2^{n-1}} \det(\frac{1}{l}B)^2$, we have

$$Q(a_1, \dots, a_{2^{n-1}}) \leq \gamma s \det\left(\frac{1}{l}B\right)^{1/2^{n-2}}.$$

Note that $\prod_{i<j}(\eta_i - \eta_j)^2 \in K$, so $y = \prod_g g\prod_{i<j}(\eta_i - \eta_j)^2 \in \mathbb{Q}$, hence is in $\mathbb{Z}$. Let q be a prime divisor of $\operatorname{osf}(a^2+4^n)$. Let $\mathfrak{q}$ be a prime of $\mathbb{Q}(\zeta_{2^n})$ above q. Then $\mathfrak{q}$ divides either the numerator or the denominator of $(a+i2^n)/(a-i2^n)$, and in fact divides it to an odd power. Since the 2^nth root of this number yields the same extension as adjoining θ, $\mathfrak{q}$ must ramify in $\mathbb{Q}(\zeta_{2^n}, \theta)/\mathbb{Q}(\zeta_{2^n})$, hence in $K(\theta)/K$. Since η has 2^n distinct conjugates over K, we have $K(\theta) = K(\eta)$. Therefore the primes above q divide the relative discriminant of η, namely $\prod(\eta_i - \eta_j)^2$, so q divides its norm to $\mathbb{Q}$, namely y. Since we are assuming $\operatorname{osf}(a^2+4^n) \geq c'(a^2+4^n)$ for some $c' > 0$, we have $\log y \geq c'' \log|a|$ for some $c'' > 0$.

Putting everything together, we find

$$\log|a| \leq A_2 + B_2 \log|a| \det\left(\frac{1}{l}B\right)^{1/2^{n-1}},$$

for some constants A_2, B_2. Therefore $\det(\frac{1}{l}B)^{-1}$ is bounded above, independently of a.

Standard index calculations show that $\det B = [S : C^l]$, and of course $[C : C^l] = l^{2^{n-1}}$. Therefore $\det(\frac{1}{l}B)^{-1}$ is the generalized index $[C : S]$. Since we already know that $[D : C]$ is bounded, we find that $[D : S]$ is bounded. This completes the proof of the theorem.

Corollary 1. *Assume* $2^n|a$. *Let* Σ *be the group of units generated by the units of Theorem* 5. *Let* $\Delta = \{u \in K(\theta) | u^l \in \Sigma$ *for some* $l > 0\}$. *Let* a *run through* *a sequence of integers such that* $(a^2+4^n)/\operatorname{osf}(a^2+4^n)$ *is bounded above. Then the index* $[\Delta : \Sigma]$ *is bounded independently of* a.

Proof. Assume the result is true for $n-1$. Write $\Sigma = \Sigma_+ \oplus \Sigma_-$, where

$$\Sigma_- = \{u \in \Sigma | \tau^{2^{n-1}}u = \pm u^{-1}\},$$

and similarly for Σ_+. Note that Σ_- is the group S in Theorem 6 and Σ_+ is the group coming from subfields.

Let $u \in \Delta$ with $u^l \in \Sigma$. Then

$$u^{2l} = (u^{(1+\tau^{2^{n-1}})})^l (u^{(1-\tau^{2^{n-1}})})^l = u_+^l u_-^l,$$

and we must have $u_\pm^l \in \Sigma_\pm$. By the induction assumption, $u_+^{l_1} \in \Sigma_+$ for some $l_1 > 0$ that is bounded independently of a. Theorem 6 implies that $u_-^{l_2} \in \Sigma_-$ for some $l_2 > 0$ that is bounded independently of a. Therefore $u^{2l_1l_2} = (u_+u_-)^{l_1l_2} \in \Sigma$. Since $2l_1l_2$ is bounded independently of a, the result follows.

7. Examples for the case $a^2 + 4^n = 2b^2$

From the proof of the irreducibility criterion of the polynomial $P_n(X; a)$, we noticed something special when $a^2 + 4^n = 2b^2$ for some integer b. In this case, $P_n(X; a)$ is irreducible in $\mathbb{Z}[X]$ and $\mathbb{Q}(\theta)$ has a quadratic subfield $\mathbb{Q}(\sqrt{2})$, where θ is any fixed root of $P_n(X; a)$. It can be seen from Theorem 4 that u_{n-1} satisfies $X^2 - \frac{a}{2^{n-1}}X - 1$ and hence $\mathbb{Q}(u_{n-1}) = \mathbb{Q}(\sqrt{a^2+4^n}) = \mathbb{Q}(\sqrt{2})$. It is in this case that $\mathbb{Q}(\theta)$ becomes Galois over the rationals for the octic field ($n = 3$), see [13]. As a matter of fact, this is the last n for which we have a family of Galois extensions over the rationals. Therefore in this section, we assume $a^2+4^n = 2b^2$ and this implies that $2^n | a$ so that $\mathbb{Q}(\theta)$ contains $\mathbb{Q}(\sqrt{2})$ and u_j's are units in the ring $\mathcal{O}_{K(\theta)}$, where $K = \mathbb{Q}(\zeta_{2^n})^+$.

From Theorem 5, we have $2^n - 1$ units

$$\{M^{2^j(k-1)}(u_j) | 1 \le k \le 2^{n-j-1} \text{ and } 0 \le j < n\}.$$

Let S be the group generated by -1 and the 2^n-1 units listed above, and call S the simplest units of $K(\theta)$. Note that $M^{2^{n-2}}(u_0) = \frac{u_0-1}{u_0+1}$ and $u_1 = \frac{u_0^2-1}{2u_0}$. So we have

$$\sqrt{u_0u_1M^{2^{n-2}}(u_0)} = \sqrt{u_0\frac{u_0^2-1}{2u_0}\frac{u_0-1}{u_0+1}} = \frac{u_0-1}{\sqrt{2}},$$

which is also a unit of $\mathcal{O}_{K(\theta)}$. Similarly, we have units of the form $\frac{M^{k-1}(u_0)-1}{\sqrt{2}}$, for $1 \le k \le 2^{n-2}$. They are all square roots of elements in S. Replace the units

$$\{M^{k-1}(u_0) | 2^{n-2} < k \le 2^{n-1}\}$$

by the units

$$\left\{\left.\frac{M^{k-1}(u_0)-1}{\sqrt{2}}\right| 1 \le k \le 2^{n-2}\right\}.$$

Do the same thing for each u_j, $1 \le j \le n-2$; and replace the units

$$\{M^{2^j(k-1)}(u_j) | 2^{n-j-2} < k \le 2^{n-j-1}\}$$

by the units

$$\left\{ \frac{M^{2^j(k-1)}(u_j)-1}{\sqrt{2}} \middle| 1 \le k \le 2^{n-j-2} \right\}.$$

So now we have another $2^n - 1$ units in the ring $\mathscr{O}_{K(\theta)}$:

$$\left\{ M^{2^j(k-1)}(u_j),\ \frac{M^{2^j(k-1)}(u_j)-1}{\sqrt{2}} \middle| 1 \le k \le 2^{n-j-2},\ 0 \le j \le n-2 \right\} \cup \{u_{n-1}\}.$$

Let S' be the group generated by -1 and the units listed above, and call S' the modified simplest units of $K(\theta)$. Clearly, S is a subgroup of S' and the index is $[S' : S] = 2^{2^{n-1}-1}$. Recall S is a subgroup of the full unit group E of the ring $\mathscr{O}_{K(\theta)}$. Assuming $[E : S]$ is finite, we have

$$[E : S'] = \frac{[E : S]}{[S' : S]} = \frac{[E : S]}{2^{2^{n-1}-1}},$$

and therefore the modified simplest units of $K(\theta)$ are closer to being a fundamental system of units than the simplest units of $K(\theta)$.

There are two special a's to which we should pay more attention in view of Lemma 2, namely $a = \pm 2^n$, and $a = \pm 2^n \cdot 239$. Note that $P_n(X; a)$ and $P_n(X; -a)$ generate the same number field. For if θ is a root of $P_n(X; a)$ then $-\theta$ is a root of $P_n(X; -a)$. This can be seen from the fact that $R_n(X)$ is an even polynomial while $I_n(X)$ is an odd polynomial. So now, let us discuss these two examples and work with the positive sign in the following.

Example 1. $a = 2^n$: Since $R_{n+1}(X) = P_n(X; 2^n)P_n(X; -2^n)$, Proposition 3 tells us that $P_n(X; 2^n)$ generates the real cyclotomic field $\mathbb{Q}(\zeta)^+$ for each n, where $\zeta = \zeta_{2^{n+2}}$. So we have a family of Galois extensions $\mathbb{Q}(\theta)$ over the rationals, where θ is any root of $P_n(X; 2^n)$. Calculation shows that

$$u_j = -i\frac{1+\zeta^{2^j}}{1-\zeta^{2^j}}, \qquad 0 \le j < n.$$

Our simplest units S are generated by -1 and the units

$$\{M^{2^j(k-1)}(u_j) | 1 \le k \le 2^{n-j-1} \text{ and } 0 \le j < n\}.$$

From the discussion above, we replace the simplest units S by the modified simplest units S'.

Our goal is to compute a system of fundamental units from the modified simplest units S'. Therefore, let us compare the modified simplest units with the cyclotomic units. The cyclotomic units $C^+_{2^{n+2}}$ of $\mathbb{Q}(\zeta)^+$ are generated by -1 and the units [15]

$$\xi_b = \zeta^{\frac{1-b}{2}} \frac{1-\zeta^b}{1-\zeta}, \qquad 3 \le b < 2^{n+1},\ b \text{ odd},$$

and $[E^+_{2^{n+2}} : C^+_{2^{n+2}}] = h^+_{2^{n+2}}$, the class number of $\mathbb{Q}(\zeta)^+$, where $E^+_{2^{n+2}}$ is the full unit group of $\mathbb{Q}(\zeta)^+$. It is easy to see that we always have

$$u_0 = \xi_{2^{n+1}-1}, \qquad \text{for each } n.$$

Let $c_k = \xi_{2k+1}$, $1 \le k \le 2^n - 1$. If $n \le 5$ then $h^+_{2^{n+2}} = 1$ (see [8]), hence $C^+_{2^{n+2}}$ is the full unit group. We consider these n. However, we skip the first two n's because of triviality.

(1) *Octic case* $(n = 3)$: $\zeta = \zeta_{32}$.
Calculation shows that

$$s_1 = c_7, \quad s_2 = \frac{c_5}{c_2}, \quad s_3 = c_3, \quad s_4 = \frac{c_1}{c_2},$$
$$s_5 = \frac{c_3c_4}{c_7}, \quad s_6 = \frac{c_1c_6}{c_7}, \quad s_7 = \frac{c_1c_2c_5c_6}{c_3c_4c_7};$$

and the index $[E : S'] = 2$. So we must have some unit in S', which is a square in E. One such unit is $s_1s_2s_4^{-2}s_5^{-1}s_6^3s_7^{-1} = c_6^2$, and therefore, the set

$$\{s_1, s_2, s_3, s_4, \sqrt{s_1s_2s_4^{-2}s_5^{-1}s_6^3s_7^{-1}}, s_6, s_7\}$$

forms a system of fundamental units of the octic field $\mathbb{Q}(\zeta_{32})^+$.

(2) 16-*tic case* $(n = 4)$: $\zeta = \zeta_{64}$.
Calculation shows that

$$s_1 = c_{15}, \quad s_2 = \frac{c_{13}}{c_2}, \quad s_3 = \frac{c_{11}}{c_4}, \quad s_4 = \frac{c_9}{c_6}, \quad s_5 = c_7, \quad s_6 = \frac{c_5}{c_2},$$
$$s_7 = \frac{c_3}{c_4}, \quad s_8 = \frac{c_1}{c_6}, \quad s_9 = \frac{c_7c_8}{c_{15}}, \quad s_{10} = \frac{c_5c_{10}}{c_2c_{13}}, \quad s_{11} = \frac{c_3c_{12}}{c_{15}}, \quad s_{12} = \frac{c_1c_{14}}{c_2c_{13}},$$
$$s_{13} = \frac{c_3c_4c_{11}c_{12}}{c_7c_8c_{15}}, \quad s_{14} = \frac{c_1c_6c_9c_{14}}{c_7c_8c_{15}}, \quad s_{15} = \frac{c_1c_2c_5c_6c_9c_{10}c_{13}c_{14}}{c_3c_4c_7c_8c_{11}c_{12}c_{15}};$$

and the index $[E : S'] = 16$. We have

$$\frac{s_1s_3s_{11}^3}{s_7^2s_9s_{13}} = c_{12}^2, \quad \frac{s_2s_8^2s_{10}s_{14}^2}{s_4s_{12}^3s_{13}s_{15}} = \left(\frac{c_{13}}{c_{14}}\right)^2, \quad \frac{s_1^2s_4^2s_9s_{12}^6s_{13}^3s_{15}^3}{s_8^4s_{10}^3s_{14}^5} = c_{14}^4;$$

and the following set forms a system of fundamental units of the 16-tic field:

$$\left\{s_1, \dots, s_8, \sqrt{\frac{s_1^2s_4^2s_9s_{12}^6s_{13}^3s_{15}^3}{s_8^4s_{10}^3s_{14}^5}}, \sqrt{\frac{s_2s_8^2s_{10}s_{14}^2}{s_4s_{12}^3s_{13}s_{15}}}, s_{11}, s_{12}, \sqrt[4]{\frac{s_1s_3s_{11}^3}{s_7^2s_9s_{13}}}, s_{14}, s_{15}\right\}.$$

(3) 32-*tic case* $(n = 5)$: $\zeta = \zeta_{128}$.
Calculation shows that

$$s_1 = c_{31}, \quad s_2 = \frac{c_{29}}{c_2}, \quad s_3 = \frac{c_{27}}{c_4}, \quad s_4 = \frac{c_{25}}{c_6}, \quad s_5 = \frac{c_{23}}{c_8}, \quad s_6 = \frac{c_{21}}{c_{10}},$$
$$s_7 = \frac{c_{19}}{c_{12}}, \quad s_8 = \frac{c_{17}}{c_{14}}, \quad s_9 = c_{15}, \quad s_{10} = \frac{c_{13}}{c_2}, \quad s_{11} = \frac{c_{11}}{c_4}, \quad s_{12} = \frac{c_9}{c_6},$$
$$s_{13} = \frac{c_7}{c_8}, \quad s_{14} = \frac{c_5}{c_{10}}, \quad s_{15} = \frac{c_3}{c_{12}}, \quad s_{16} = \frac{c_1}{c_{14}}, \quad s_{17} = \frac{c_{15}c_{16}}{c_{31}},$$
$$s_{18} = \frac{c_{13}c_{18}}{c_2c_{29}}, \quad s_{19} = \frac{c_{11}c_{20}}{c_4c_{27}}, \quad s_{20} = \frac{c_9c_{22}}{c_6c_{25}}, \quad s_{21} = \frac{c_7c_{24}}{c_{31}},$$
$$s_{22} = \frac{c_5c_{26}}{c_2c_{29}}, \quad s_{23} = \frac{c_3c_{28}}{c_4c_{27}}, \quad s_{24} = \frac{c_1c_{30}}{c_6c_{25}}, \quad s_{25} = \frac{c_7c_8c_{23}c_{24}}{c_{15}c_{16}c_{31}},$$
$$s_{26} = \frac{c_5c_{10}c_{21}c_{26}}{c_2c_{13}c_{18}c_{29}}, \quad s_{27} = \frac{c_3c_{12}c_{19}c_{28}}{c_{15}c_{16}c_{31}}, \quad s_{28} = \frac{c_1c_{14}c_{17}c_{30}}{c_2c_{13}c_{18}c_{29}},$$
$$s_{29} = \frac{c_3c_4c_{11}c_{12}c_{19}c_{20}c_{27}c_{28}}{c_7c_8c_{15}c_{16}c_{23}c_{24}c_{31}}, \quad s_{30} = \frac{c_1c_6c_9c_{14}c_{17}c_{22}c_{25}c_{30}}{c_7c_8c_{15}c_{16}c_{23}c_{24}c_{31}},$$
$$s_{31} = \frac{c_1c_2c_5c_6c_9c_{10}c_{13}c_{14}c_{17}c_{18}c_{21}c_{22}c_{25}c_{26}c_{29}c_{30}}{c_3c_4c_7c_8c_{11}c_{12}c_{15}c_{16}c_{19}c_{20}c_{23}c_{24}c_{27}c_{28}c_{31}};$$

and the index $[E : S'] = 2048$. We have

$$\begin{aligned}
c_{24}^2 &= s_1 s_5 s_{13}^{-2} s_{17}^{-1} s_{21}^3 s_{25}^{-1}, \\
c_{25}^2 c_{30}^{-2} &= s_4 s_8^{-1} s_{16}^2 s_{20} s_{24}^{-3} s_{26}^{-1} s_{28}^2 s_{29} s_{30}^{-2} s_{31}, \\
c_{26}^2 c_{29}^{-2} &= s_2^{-1} s_6 s_{14}^{-2} s_{18}^{-1} s_{22}^3 s_{26}^{-1}, \\
c_{27}^2 c_{28}^2 &= s_1^2 s_3 s_7 s_{15}^{-2} s_{17} s_{19}^{-2} s_{23}^3 s_{25}^2 s_{27}^{-3} s_{29}^2, \\
c_{28}^4 &= s_1^2 s_7^2 s_{15}^{-4} s_{17} s_{19}^{-3} s_{23}^6 s_{25}^3 s_{27}^{-5} s_{29}^3, \\
c_{29}^4 c_{30}^4 &= s_1^4 s_2^2 s_8^2 s_{16}^{-4} s_{17}^2 s_{18}^{-1} s_{20}^{-3} s_{24}^6 s_{25} s_{26}^2 s_{28}^{-5} s_{29}^{-2} s_{30}^5 s_{31}^{-2}, \\
c_{30}^8 &= s_1^4 s_8^4 s_{16}^{-8} s_{17}^2 s_{20}^{-6} s_{24}^{12} s_{25} s_{26}^5 s_{28}^{-10} s_{29}^{-5} s_{30}^{11} s_{31}^{-5},
\end{aligned}$$

and therefore the set

$$\left\{ s_1, s_2, s_3, \frac{c_{25}}{c_{30}}, c_{24}, \frac{c_{26}}{c_{29}}, \frac{c_{27}}{c_{28}}, s_8, \ldots, s_{16}, c_{28}, \frac{c_{29}}{c_{30}}, \right.$$
$$\left. s_{19}, \ldots, s_{24}, c_{30}, s_{26}, \ldots, s_{31} \right\}$$

forms a system of fundamental units of the 32-tic field $\mathbb{Q}(\zeta_{128})^+$.

These examples indicate that S' and hence S should always be a subgroup of C^+, where $C^+ = C^+_{2^{n+2}}$; and the index $[C^+ : S']$ is 2^1, 2^{1+3}, 2^{1+3+7} for $n = 3, 4, 5$ respectively. We may conjecture that the exponent of this index is

$$1 + 3 + 7 + \cdots + (2^{n-2} - 1) = \sum_{k=3}^{n} (2^{k-2} - 1) = 2^{n-1} - n,$$

and therefore for $n \geq 3$ we have (note that it is also true for $n = 1, 2$)

$$[C^+ : S'] = 2^{2^{n-1} - n}.$$

Since $[S' : S] = 2^{2^{n-1}-1}$ and $[E^+ : C^+] = h^+$, where $E^+ = E^+_{2^{n+2}}$ and $h^+ = h^+_{2^{n+2}}$; we conclude that

$$[E^+ : S] = 2^{2^n - n - 1} \cdot h^+$$

and state it as a conjecture in the following.

Conjecture 1. The simplest units have index $2^{2^n - n - 1} \cdot h^+$ in the full unit group of $\mathcal{O}_{\mathbb{Q}(\zeta_{2^{n+2}})^+}$, for $a = \pm 2^n$, $n \geq 1$.

Example 2. $a = 2^n \cdot 239$: Since $a^2 + 4^n = 2 \cdot 13^4 \cdot 4^n$, the field $\mathbb{Q}(\theta)$ contains the quadratic field $\mathbb{Q}(\sqrt{2})$ as expected, where θ is any fixed root of $P_n(X; 2^n \cdot 239)$. We know that $\mathbb{Q}(\theta)$ is Galois over the rationals when $n \leq 3$. For $n = 4$, our ε in Theorem 1 is $1 + \sqrt{2} + \sqrt{4 + 2\sqrt{2}}$ (see Proposition 2). By Theorem 4, $\mathbb{Q}(\theta)$ contains a quartic subfield $\mathbb{Q}(u_2)$, where u_2 is a root of the polynomial

$$X^4 - 4 \cdot 239 X^3 - 6X^2 + 4 \cdot 239 X + 1.$$

One such u_2 is $239 + 169\sqrt{2} + 13(7 + 5\sqrt{2})\sqrt{4 + 2\sqrt{2}}$, and hence $\sqrt{4 + 2\sqrt{2}}$ belongs to the field $\mathbb{Q}(\theta)$. Thus $\varepsilon \in \mathbb{Q}(\theta)$, and we conclude that $\mathbb{Q}(\theta)$ is Galois over the rationals. Calculation shows that the conductor f of this field is $64 \cdot 13$, and its discriminant d is $2^{79} \cdot 13^{12}$. When $n \geq 5$, the extension $\mathbb{Q}(\theta)/\mathbb{Q}$ is not Galois, so the above example completes the list of Galois extensions we obtain by our methods.

References

1. J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer-Verlag, Berlin, 1959.
2. G. Cornell and L. C. Washington, *Class numbers of cyclotomic fields*, J. Number Theory **21** (1985), 260–274.
3. Marie-Nicole Gras, *Special units in real cyclic sextic fields*, Math. Comp. **48** (1987), 179–182.
4. ——, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de* $\mathbb{Q}$, Publ. Math. Besançon, 1977-1978, fasc. 2, 53 pp.
5. Andrew J. Lazarus, *The class number and cyclotomy of simplest quartic fields*, Ph.D. thesis, Univ. of California, Berkeley, 1989.
6. ——, *Class numbers of simplest quartic fields*, Number Theory (R. A. Mollin, ed.), De Gruyter, Berlin and New York, 1990, pp. 313–323.
7. ——, *On the class number and unit index of simplest quartic fields*, Nagoya Math. J. **121** (1991), 1–13.
8. F. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), 693–707.
9. W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid.-Akad. Oslo I (N.S.) no. 5 (1942), 27 pp.
10. René Schoof and L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543–556.
11. D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.
12. Y.-Y. Shen, *Units of real cyclic octic fields*, Ph.D. thesis, Univ. of Maryland at College Park, 1988.
13. ——, *Unit groups and class numbers of real cyclic octic fields*, Trans. Amer. Math. Soc. **326** (1991), 179–209.
14. R. Steiner and N. Tzanakis, *Simplifying the solution of Ljunggren's equation* $X^2+1 = 2Y^4$, J. Number Theory **37** (1991), 123–132.
15. L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., vol. 83, Springer-Verlag, New York, 1982.

Department of Mathematics, The Catholic University of America, Washington, D.C. 20064

Current address: Department of Mathematics, Tunghai University, Taichung, Taiwan 407, Republic of China

E-mail address: `shen@cua.edu`

Department of Mathematics, University of Maryland, College Park, Maryland 20742

E-mail address: `lcw@amalie.umd.edu`